What is claimed:

1. A method of redirecting data items from a messaging host system to a user's mobile device, comprising the steps of:

detecting a new data item for the user at the messaging host system;

forwarding a copy of the new data item to a redirector host system;

determining whether the new data item should be redirected from the redirector host system to the user's mobile device; and

if the new data item should be redirected, then

encrypting the new data item to form an encrypted new data item; and

packaging the encrypted new data item into an electronic envelope and transmitting the electronic envelope to the user's mobile device.

2. The method of claim 1, further comprising the step of:

storing the new data item in a user's inbox coupled to the messaging host system.

3. The method of claim 1, wherein the detecting step includes the steps of:

determining whether a new data item has been received at the messaging host system for a particular user; and

checking a forwarding file coupled to the messaging host system to determine whether the particular user's data items should be redirected to the redirector host system.

4. The method of claim 3, wherein the forwarding file includes a list of system addresses where the user's data items should be forwarded by the messaging host system.

5. The method of claim 1, further comprising the steps of:

providing an inbox for the user, wherein the inbox is coupled to the messaging host system; and

forwarding a copy of the new data item to the user's inbox on the messaging host system.

6. The method of claim 1, further comprising the steps of:

configuring a set of filtering rules for use by the redirector host system in determining whether the new data item should be redirected to the user's mobile device; and

providing an access mechanism that allows the user to remotely configure and reconfigure the set of filtering rules.

7. The method of claim 1, further comprising the steps of:

configuring a user profile database for use by the redirector host system in determining whether the new data item should be redirected to the user's mobile data device; and

providing an access mechanism that allows a system administrator of the messaging host system to remotely configure and reconfigure the user profile database.

8. The method of claim 1, further comprising the steps of:

receiving the electronic envelope at the user's mobile device;

extracting the encrypted new data item from the electronic envelope; and

decrypting the encrypted new data item to recover the new data item.

9. The method of claim 8, further comprising the step of :

storing the new data item within a memory of the mobile device.

10. The method of claim 8, wherein the decrypting step comprises the step of:

using a cipher algorithm and a decryption key to decrypt the encrypted new data item.

11. The method of claim 10, further comprising the steps of:

generating the decryption key at the redirector host system; and

forwarding the decryption key from the redirector host system to the mobile device using a secure communications link.

12. The method of claim 11, wherein the step of forwarding the decryption key comprises:

forwarding the decryption key to the mobile device using Internet Message Access Protocol (IMAP) over Secure Sockets Layer (SSL) protocol.

13. The method of claim 10, wherein the encrypting step comprises the step of:

using a cipher algorithm and an encryption key to encrypt the new data item.

14. The method of claim 13, further comprising the steps of:

generating the encryption key at the redirector host system;

storing the encryption key at the redirector host system;

generating the decryption key at the redirector host system; and

forwarding the decryption key from the redirector host system to the mobile device using a secure communications link.

15. The method of claim 13, further comprising the steps of:

generating a private key to be used as the decryption key at the redirector host system;

forwarding the private key from the redirector host system to the mobile device using a secure communications link;

generating a public key to be used as the encryption key at the redirector host system; and

forwarding the public key from the redirector host system to a public key repository.

16. The method of claim 15, wherein the step of forwarding the private key comprises:

forwarding the private key to the mobile device using Internet Message Access Protocol (IMAP) over Secure Sockets Layer (SSL) protocol.

17. The method of claim 13, further comprising the steps of:

generating the encryption key at a computer system associated with the mobile device;

forwarding the encryption key from the computer system to the redirector host system using a secure communications link;

generating the decryption key at the computer system associated with the mobile device; and

forwarding the decryption key from the computer system to the mobile device using a secure communications link.

18. The method of claim 17, wherein the step of forwarding the decryption key comprises:

sending the decryption key to the mobile device over a serial connection between the computer system and the mobile device.

19. The method of claim 13, further comprising the steps of:

generating a private key to be used as the decryption key at a computer system associated with the mobile device;

forwarding the private key from the redirector host system to the mobile device using a secure communications link;

generating a public key to be used as the encryption key at the computer system; and

forwarding the public key from the computer system to a public key repository.

20. The method of claim 19, further comprising the step of:

forwarding the public key from the computer system to the redirector host system.

21. The method of claim 13, further comprising the steps of:

generating the encryption key at the mobile device;

forwarding the encryption key from the mobile device to the redirector host system using a secure communications link;

generating the decryption key at the mobile device;

storing the decryption key at the mobile device.

22. The method of claim 13, further comprising the steps of:

generating a private key to be used as the decryption key at the mobile device;

storing the private key at the mobile device;

generating a public key to be used as the encryption key at the mobile device; and

forwarding the public key from the mobile device to a public key repository.

23. The method of claim 22, further comprising the step of:

forwarding the public key from the mobile device to the redirector host system.

24. The method of claim 1, further comprising the steps of:

preparing a reply data item at the mobile device that is related to the new data item;

encrypting the reply data item at the mobile device to form an encrypted reply data item; and

packaging the encrypted reply data item into an electronic envelope and transmitting the electronic envelope to the redirector host system.

25. The method of claim 24, wherein the electronic envelope packaged with the encrypted reply data item is addressed using an electronic address of the redirector host system.

26. The method of claim 25, further comprising the steps of:

extracting the encrypted reply data item from the electronic envelope at the redirector host system;

decrypting the extracted, encrypted reply data item to recover the reply data item;

reconfiguring addressing information associated with the reply data item; and

transmitting the reconfigured reply data item to the messaging host system.

27. The method of claim 26, further comprising the steps of:

receiving the reconfigured reply data item at the messaging host system; and

storing the reply data item in a user's inbox coupled to the messaging host system.

28. The method of claim 25, further comprising the steps of:

extracting the encrypted reply data item from the electronic envelope at the redirector host system;

decrypting the extracted, encrypted reply data item to recover the reply data item;

reconfiguring addressing information associated with the reply data item; and

transmitting the reconfigured reply data item to a destination system using an electronic address included in the reply data item.

29. The method of claim 1, further comprising the steps of:

providing the user's mobile device with an interface to a wireless data network;

forwarding the electronic envelope from the redirector host system to a wireless gateway system; and

transmitting the electronic envelope from the wireless gateway system to the user's mobile device using the wireless data network.

30. The method of claim 1, further comprising the steps of:

transmitting a deactivation message from the user to the redirector host system; and

upon receiving the deactivation message, prohibiting the redirection of data items for the user sending the deactivation message.

31. The method of claim 1, wherein the determining step includes the steps of:

accessing a user profile database including a list of authorized users; and

checking whether the user associated with the new data item is an authorized user to determine whether the new data item should be redirected to the user's mobile device.

32. The method of claim 1, wherein the determining step includes the steps of:

accessing a filter rules database including a list of filters to be applied to data items for a particular user; and

applying the filters to the new data item to determine whether the new data item should be redirected to the user's mobile device.

33. The method of claim 1, wherein the packaging step includes the step of addressing the electronic envelope using the electronic address of the user's mobile device.

34. The method of claim 1, wherein the data items are E-mail messages, and wherein the messaging host system is an E-mail host system.

35. The method of claim 1, wherein the user's mobile device is a laptop computer.

36. The method of claim 1, wherein the user's mobile device is a two-way paging computer.

37. The method of claim 36, wherein the two-way paging computer includes a wireless network interface for communicating with the redirector host system via a wireless data network.

38. The method of claim 37, wherein the redirector host system is coupled to the wireless data network via a wireless gateway system.

39. The method of claim 38, wherein the electronic envelope is addressed using the wireless data network address of the two-way paging computer.

40. The method of claim 1, wherein the messaging host system is an Internet Service Provider.

41. The method of claim 40, wherein the data items are E-mail messages, and wherein the Internet Service Provider includes a mail server program.

42. The method of claim 41, wherein the Internet Service Provider further includes a forwarding database coupled to the mail server program for detecting whether a new data item received at the mail server should be forwarded to a redirector host system, and for determining the electronic address of that redirector host system.

43. The method of claim 1, wherein the messaging host system and the redirector host system are coupled via the Internet.

44. The method of claim 1, wherein the redirector host system includes a further messaging host system.

45. The method of claim 1, wherein the redirector host system is incorporated with the messaging host system.

46. The method of claim 6, wherein the access mechanism for remotely configuring and reconfiguring the filtering rules is a web-page interface.

47. The method of claim 7, wherein the access mechanism for remotely configuring and reconfiguring the user profile database is a web-page interface.

48. The method of claim 1, further comprising the steps of:

configuring a user profile database for use by the redirector host system in determining whether the new data item should be redirected to the user's mobile data device; and

storing, within the user profile database, the electronic address of the user's mobile device.

49. The method of claim 48, further comprising the step of:

storing, within the user profile database, information regarding the type and configuration of the user's mobile device.

50. The method of claim 1, wherein the packaging step further includes the steps of:

converting the encrypted new data item into a compressed format; and

placing the compressed new data item into an electronic envelope that is addressed using the electronic address of the user's mobile device.

51. A method of redirecting E-mail messages from a messaging host system to a user's wireless mobile device, comprising the steps of:

detecting an E-mail message for the user at the messaging host system;

forwarding a copy of the E-mail message from the messaging host system to a wireless redirector host system;

receiving the forwarded E-mail message at the wireless redirector host system and applying a set of user-defined filtering rules that determine whether or not to redirect the E-mail to the user's wireless mobile device via a wireless network coupled to the wireless redirector host system; and

if the filtering rules determine that the E-mail message is of the type that should be redirected, then encrypting the E-mail message to form an encrypted E-mail message and redirecting the encrypted E-mail message to the user's wireless mobile device by packaging the encrypted E-mail message in an electronic envelope that includes a wireless network address of the user's wireless mobile device.

52. The method of claim 51, further comprising the steps of:

providing a filter rules database for storing the user-defined filter rules; and

providing an interface mechanism coupled to the filter rules database through which the user may define and re-define the filtering rules.

53. The method of claim 52, wherein the interface mechanism is a web page interface.

54. The method of claim 53, wherein the web page interface includes an activation/deactivation switch for turning on/off the operation of the wireless redirector host system for a particular user.

55. The method of claim 51, further comprising the step of:

accessing a user profile database coupled to the wireless redirector host system to verify that the user associated with the E-mail message is an authorized user.

56. The method of claim 55, further comprising the step of:

providing an access mechanism that allows a system administrator of the messaging host system to remotely configure and reconfigure the user profile database.

57. The method of claim 51, wherein the messaging host system is an Internet Service Provider (ISP).

58. The method of claim 57, wherein the ISP and the wireless redirector host system communicate via the Internet.

59. The method of claim 51, wherein the wireless redirector host system and the wireless mobile device communicate through a wireless gateway system and a wireless communication network.

60. A system for redirecting data items from a network to a user's wireless mobile device, comprising:

a messaging host system coupled to the network for receiving data items associated with a particular user and for forwarding the received data items to a predetermined address on the network; and

a redirector host system associated with the predetermined address for receiving the forwarded data items from the messaging host system and for encrypting and redirecting the forwarded data items to the user's wireless mobile device.

61. The system of claim 60, wherein the network is the Internet.

62. The system of claim 60, wherein the messaging host system further includes:

a sendmail program for receiving and transmitting user data items; and

a forwarding file containing a list of authorized users of the system and the predetermined address.

63. The system of claim 60, wherein the redirector host system comprises an encryption module that encrypts the forwarded data items from the messaging host system.

64. The system of claim 63, wherein the encryption module uses a cipher algorithm and an encryption key to encrypt the forwarded data items.

65. The system of claim 64, wherein the wireless mobile device includes a decryption module that decrypts encrypted data items redirected to the mobile device.

66. The system of claim 65, wherein the decryption module uses a cipher algorithm and a decryption key to decrypt the encrypted data items.

67. The system of claim 66, wherein the redirector host system further comprises:

means for generating the encryption key and the decryption key;

means for storing the encryption key; and

means for forwarding the decryption key to the mobile device using a secure communications link.

68. The system of claim 67, wherein the mobile device further comprises:

means for receiving the decryption key forwarded by the redirector host system; and

means for storing the decryption key.

69. The system of claim 67, wherein the encryption key is a public key and the decryption key is a private key.

70. The system of claim 66, wherein the mobile device further comprises:

means for generating the encryption key and the decryption key;

means for forwarding the encryption key to the redirector host system using a secure communications link; and

means for storing the decryption key.

71. The system of claim 62, wherein the messaging host system further includes a local data store for storing the data items of user's having accounts on the messaging host system.

72. The system of claim 60, wherein the redirector host system further includes:

a redirector software program for determining whether certain data items should be redirected to the user's wireless mobile device;

a filter rules database containing filtering rules to apply to the received data items for a particular user; and

a user profile database containing a list of authorized users.

73. The system of claim 72, wherein the redirector host system further includes a wireless data store for storing the forwarded data items.

74. The system of claim 60, wherein the data items are E-mail messages and the messaging host system is an E-mail server.

75. The system of claim 60, further comprising:

a wireless gateway system coupled to the redirector host system and a wireless data network for receiving the redirected data items and for transmitting those data items to the user's wireless mobile device via the wireless data network.

76. The system of claim 60, further comprising:

a filter rules database containing filtering rules to apply to the data items forwarded to the redirector host system, the filtering rules setting forth a list of data item characteristics that determine whether the redirector host system will redirect the data item.

77. The system of claim 76, further comprising:

an interface document coupled to the filter rules database for enabling the remote configuration of the filtering rules for a particular user.

78. The system of claim 77, wherein the interface document is a web page.

79. The system of claim 60, wherein the redirector host system is integrated with a second messaging host system.

80. The system of claim 60, further comprising a plurality of messaging host systems coupled to the network for receiving data items associated with particular users and for forwarding the received data items to the predetermined address, wherein the redirector host system receives the forwarded data items from the plurality of messaging host systems and encrypts and redirects those data items to each user's wireless mobile device.

81. A method of operating a host system configured to redirect E-mail messages from the Internet to a user's wireless mobile device, comprising the steps of:

receiving an E-mail message from the Internet for a particular user;

accessing a user profile database to determine whether the particular user is an authorized user of the host system;

if the user is an authorized user of the host system, then accessing a filter rules database to apply a set of user-defined filtering rules to the E-mail message that determine whether the E-mail message is the type of message that the user wants to have redirected to its wireless mobile device; and

if the filtering rules determine that the E-mail message should be redirected, then encrypting the E-mail message and repackaging the encrypted E-mail message into an electronic envelope including the address of the user's wireless mobile device and forwarding the electronic envelope to a wireless gateway system for transmission onto a wireless data network associated with the user's wireless mobile device.

82. A method for redirecting messages between an Internet Service Provider (ISP) host system and a plurality of mobile devices, the method comprising the steps of:

configuring redirection settings for one or more mobile device users at the ISP host system;

receiving incoming messages directed to a first address at the ISP host system from a plurality of message senders;

in response to the redirection settings, continuously encrypting and redirecting the incoming messages from the ISP host system to the mobile device via a redirector host system;

receiving encrypted outgoing messages generated and encrypted at the mobile communications device at the redirector host system;

decrypting the received encrypted outgoing messages to recover the outgoing messages;

configuring address information of the outgoing messages so that the first address is used as an originating address of the outgoing messages; and,

transmitting the configured outgoing messages to message recipients.

83. A method of redirecting electronic data items from a host system associated with a user to the user's mobile data communication device, comprising the steps of:

configuring an external redirection event at the host system, wherein the external redirection event is the host system sensing whether the user is in the physical vicinity of the host system;

receiving electronic data items at the host system; and

if the host system senses that the user is not in the physical vicinity of the host system, then continuously encrypting the electronic data items and redirecting the encrypted data items to the user's mobile data communication device until the host system senses that the user is in the vicinity of the host system.

84. The method of claim 83, wherein the sensing is achieved by a heat sensor detecting a lack of heat emitted by the user.

85. The method of claim 83, wherein the sensing is achieved by a motion sensor detecting a lack of motion by the user.

86. The method of claim 83, wherein the sensing is achieved by removal of the mobile device from a mobile device cradle connected to the host system.

87. In a system for redirecting data items between a host system and a mobile communications device through a redirector system, a method of key distribution comprising the steps of:

generating an encryption key for encrypting data items to be redirected to the mobile device;

generating a decryption key for decrypting encrypted and redirected data items received at the mobile device; and

forwarding the decryption key to the mobile device using a secure communications link.

88. The method of claim 87, wherein:

the steps of generating the encryption key and generating the decryption key are performed at the redirector system; and

the method further comprises the steps of forwarding the encryption key to the redirector system and storing the encryption key in a memory in the redirector system.

89. The method of claim 88, wherein the step of forwarding the decryption key to the mobile device comprises the step of:

forwarding the decryption key to the mobile device using Internet Message Access Protocol (IMAP) over Secure Sockets Layer (SSL).

90. The method of claim 87, wherein:

the steps of generating the encryption key and generating the decryption key are performed at the host system; and

the method further comprises the step of forwarding the encryption key to the redirector system using a secure communications link.

91. The method of claim 87, wherein:

the steps of generating the encryption key and generating the decryption key are performed at a computer system operatively connected to the host system; and

the method further comprises the step of forwarding the encryption key to the redirector system using a secure communications link.

92. The method of claim 91, wherein:

the secure communications link over which the decryption key is forwarded comprises a physical connection between the mobile device and the computer system.

93. The method of claim 87, wherein:

the encryption key and the decryption key are private keys; and

the method further comprises the step of forwarding the encryption key to the redirector system using a secure communications link.

94. The method of claim 87, wherein:

the encryption key is a public key;

the decryption key is a private key; and

the method further comprises the step of forwarding the encryption key to a public key repository.

95. The method of claim 87, wherein:

the host system is a messaging system; and

the data items are E-mail messages.

96. The method of claim 87, further comprising the steps of:

generating a second encryption key for encrypting data items to be sent from the mobile device;

generating a second decryption key for decrypting encrypted data items received at the redirector system from the mobile device; and

forwarding the second decryption key to the redirector system using a secure communications link.

97. In a system for redirecting data items between a host system and a mobile communications device through a redirector system, a key distribution sub-system comprising:

means for generating an encryption key for encrypting data items prior to redirection to the mobile device;

means for generating a decryption key for decrypting encrypted and redirected data items received at the mobile device; and

means for forwarding the decryption key to the mobile device using a secure communications link.

98. The system of claim 97, wherein

the key distribution system is implemented at the redirector system; and

the redirector system further comprises means for storing the encryption key.

99. The system of claim 98, wherein:

the means for forwarding the decryption key to the mobile device is configured for using Internet Message Access Protocol (IMAP) over Secure Sockets Layer (SSL).

100. The system of claim 97, wherein:

the key distribution system is implemented in a computer system operatively connected to the host system.

101. The system of claim 100, wherein:

the computer system further comprises means for forwarding the encryption key to the redirector system using a secure communications link.

102. The system of claim 100, wherein:

the encryption key is a public key; and

the computer system further comprises means for forwarding the encryption key to a public key repository.

103. The method of claim 100, wherein:

the secure communications link over which the decryption key is forwarded comprises a physical connection between the mobile device and the computer system.

104. The system of claim 97, further comprising:

means for generating a second encryption key for encrypting data items to be sent from the mobile device;

means for generating a second decryption key for decrypting encrypted data items received at the redirector system from the mobile device; and

means for forwarding the second decryption key to the redirector system using a secure communications link.